IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

AUTHENTICOM, INC., Plaintiffs, v. CDK GLOBAL, LLC, and THE REYNOLDS AND REYNOLDS COMPANY, Defendants.	No. 3:17-CV-318-JDP

DEFENDANT THE REYNOLDS AND REYNOLDS COMPANY'S MEMORANDUM IN SUPPORT OF ITS MOTION TO DISMISS PLAINTIFF AUTHENTICOM, INC.'S ORIGINAL COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

Defendant The Reynolds and Reynolds Company ("Reynolds") moves to dismiss Plaintiff Authenticom, Inc.'s ("Authenticom") Original Complaint pursuant to Federal Rule of Civil Procedure 12(b)(6). In support of that motion, Reynolds would show as follows:

I. INTRODUCTION

This lawsuit is an effort to achieve sanctuary in this Court for Authenticom's illegal conduct. But the Supreme Court and Congress have already made the determination: the law will not allow it. Authenticom's claims must be dismissed.

Authenticom's business model is to enter Reynolds' proprietary computer system, admittedly without Reynolds' authorization and in contravention of Reynolds' license agreements, take the data it wants for free, and sell that data to others. Authenticom *pleads* it has engaged in this computer abuse and trespassing, bragging about its methods of working around Reynolds' system security. *See e.g.*, Orig. Compl. ¶¶ 195, 197, 199 [Dkt. 1] (hereinafter "Compl."). Such conduct is illegal under a host of statutes and authorities, as further outlined below and in Reynolds' separately filed counterclaims. Reynolds files this motion because that illegality is outcome determinative: the antitrust laws do not countenance "victims" who engage in such illegal behavior, nor do they condemn others' efforts to block it.

Authenticom seeks to accomplish through legal action what it could not through technology. But Reynolds has a clearly established right to choose who it does business with, and more specifically, who has access to its systems and software. The United States Supreme Court has affirmed that right, as has Congress—the former through its *Trinko* decision (and progeny), and the latter through the Computer Fraud and Abuse Act. For over a decade, Reynolds has legally exercised that right in its customer licensing agreements, which limit system access and use solely to Reynolds' customers and their employees. Reynolds' actions to defend that choice and those rights are equally legal. That is especially true with respect to third

parties like Authenticom, which is neither a customer nor supplier of Reynolds' system—but instead acts solely as an interloper seeking to glom onto the system for free for its own profit.

To escape the inexorable conclusion that its business practices are illegal, Authenticom attempts to plead a horizontal conspiracy claim against Reynolds and its largest and fiercest competitor, CDK. In doing so, it stumbles immediately by alleging a "key" clause that in fact does not exist. The actual agreement between CDK and Reynolds is far more limited: it provides only that the parties would engage in an orderly wind-down of CDK's (equally illegal) practice of unauthorized access to Reynolds' DMS. Nothing about that is an antitrust violation as a matter of law.

Perhaps in anticipation of this problem, Authenticom spins a series of broader conspiracy theories, the thrust of which is that Reynolds and CDK agreed to destroy Authenticom. But Authenticom cannot escape its own facts, admitting that (1) Reynolds had not allowed data integrators access to its system for more than a decade before the supposed conspiracy; (2) Reynolds had long taken a public stance against hostile integration, including in public court filings and cease-and-desist letters; (3) Reynolds was successfully blocking CDK's own data-integration arm from accessing its system; (4) Reynolds has never participated in the "data integration market" with respect to CDK's or any other DMS providers' enterprise systems; and (5) Reynolds continues to use Authenticom's non-hostile integration services for other DMS providers. Those facts, individually and in combination, defeat the plausibility of Authenticom's theories. Authenticom plausibly alleges only that CDK agreed to cease its equally-forbidden accessing of Reynolds' DMS without authorization. That is not an antitrust violation. To hold otherwise would be to hold that CDK was prohibited from agreeing to cease illegal activity.

Authenticom's other antitrust causes of actions are equally flawed. And of course, its tortious interference claims are based upon contracts that call for illegal performance, which, like its antitrust theories based on the same premise, cannot survive as a matter of law.

Authenticom's use of the Courts in an effort to sanction its illegal conduct should not stand. Each of Authenticom's claims should be dismissed with prejudice.

II. SUMMARY OF ALLEGED FACTS[1]

Reynolds produces, supports, and licenses enterprise computer systems to car dealerships that assist them in managing their business. *See* Compl. ¶¶ 2-3, 28-29, 39. These systems are known as Dealer Management Systems, or "DMSs." *See id.* ¶ 3. Authenticom's allegations set forth its ongoing efforts to access Reynolds' proprietary DMS computer systems, extract data, and sell it to third party vendors who in turn resell their services to dealers. *See id.* ¶¶ 77, 82, 92, 189. Authenticom admits that Reynolds has consistently opposed Authenticom's and others' attempts to access Reynolds' systems in this manner without authorization. *See id.* ¶¶ 6, 74, 92, 103, 106-107, 109, 185. Reynolds effected this opposition contractually, through legal action, and technologically. *See id.*

Authenticom claims that Reynolds adopted this approach beginning in 2007 and that its subsequent technological blocking efforts have become increasingly effective. *See id.* Authenticom alleges that these restrictions harmed its business because, without direct access to the DMS, Authenticom's ability to provide data from automated access to Reynolds' systems to other parties for profit has suffered. *See, e.g.*, *id.* ¶ 14. Authenticom admits, however, that

[1] The facts set forth herein are based on Authenticom's Complaint, which must be accepted as true except where they are contradicted by a cited contract or other central document. *See* Sections III(A) and (B), *infra*. Nothing in this Motion is intended to concede the truth of any facts alleged.

dealers can still send data without providing access to Reynolds' systems in other ways—albeit less efficiently. *See id.* ¶ 105.

Authenticom further alleges that in 2015, Reynolds entered into an agreement with CDK in which CDK agreed that it would cease accessing Reynolds' DMS without authorization, quoting a provision that does not appear in that agreement. *Compare* Compl. ¶ 134 *with* Ex. 4. At the time of the agreement, CDK owned a subsidiary that had historically engaged in unauthorized access to the DMS and sale of the fruits of that access to others just as Authenticom had. *See id.* ¶¶ 7, 58, 93. Authenticom admits that efforts by CDK's affiliate to access Reynolds' systems were also thwarted by Reynolds' technological measures. *See* Compl. ¶¶ 6-92. According to Authenticom, it learned of this agreement from Reynolds in April 2015. *See id.* ¶ 181. Authenticom filed this lawsuit two years later.

III. ARGUMENT AND AUTHORITIES

A. The Rule 12(b)(6) Standard

In evaluating whether a claim can survive under Rule 12(b)(6), the Court must evaluate whether a plaintiff has pleaded claims that are supported by plausible factual allegations and that are legally cognizable. *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007). The court must treat all well-pleaded facts as true, draw reasonable inferences in the plaintiff's favor, and generally read the complaint in the light most favorable to the plaintiff. *See generally id.* On the other hand, legal conclusions are not entitled to the same presumption. A plaintiff cannot rely on "labels and conclusions," and the court is not bound to accept legal conclusions couched as factual allegations. *See id.* at 555; *Tamayo v. Blagojevich*, 526 F.3d 1074, 1092 (7th Cir. 2008).

In addition, "a party may plead itself out of court by either including factual allegations that establish an impenetrable defense to its claims or by attaching exhibits that establish the same." *Massey v. Merrill Lynch & Co., Inc.*, 464 F.3d 642, 650 (7th Cir. 2006). "A plaintiff

pleads himself out of court when it would be necessary to contradict the complaint in order to prevail on the merits." *Tamayo*, 526 F.3d at 1086 (internal marks omitted). This rule extends to affirmative defenses such as limitations and laches as well: "While complaints typically do not address affirmative defenses, the statute of limitations may be raised in a motion to dismiss if the allegations of the complaint itself set forth everything necessary to satisfy the affirmative defense." *Brooks v. Ross*, 578 F.3d 574, 579 (7th Cir. 2009) (internal marks omitted).

The fundamental purpose of Rule 12(b)(6) is to protect defendants from the burden of responding to meritless theories and claims. As Judge Posner stated, "*Twombly*, even more clearly than its successor, [*Iqbal*], is designed to spare defendants the expense of responding to bulky, burdensome discovery unless the complaint provides enough information to enable an inference that the suit has sufficient merit to warrant putting the defendant to the burden of responding to at least a limited discovery demand." *In re Text Messaging Antitrust Litig.*, 630 F.3d 622, 625 (7th Cir. 2010). This is particularly true in the antitrust context because "[a]ntitrust claims are expensive to defend and thus offer plaintiffs a large degree of leverage in settlement discussions." *Texas Ujoints LLC v. Dana Holding Corp.*, 13-C-1008, 2014 WL 4443276, at *3 (E.D. Wis. Sept. 9, 2014).

B. The Court Can Consider Additional Documents, Including the Pleaded Contracts

In addition to the complaint itself, this Court can also consider documents that are referred to in the complaint, are concededly authentic, and are central to the plaintiff's claims. *See Santana v. Cook Cty. Bd. of Review*, 679 F.3d 614, 619 (7th Cir. 2012); *see also Hecker v. Deere & Co.*, 556 F.3d 575, 582 (7th Cir. 2009) (stating that the Seventh Circuit has been "relatively liberal" in considering outside documents). This case involves at least three sets of documents that satisfy these criteria: 1) Reynolds' DMS contracts with its dealership customers;

2) Reynolds' RCI contracts; and 3) the February 2015 agreement Authenticom alleges is a horizontal conspiracy. All three groups of contracts are expressly referenced (and in some cases quoted) in Authenticom's Complaint[2] and indisputably form a core part of its claims. Indeed, Authenticom is expressly asking the Court to invalidate provisions within the first two groups of contracts (*see* Compl. ¶¶ 89-90), and Authenticom's horizontal conspiracy claim is based upon the third set of agreements.

There is also no dispute as to the authenticity of the attached agreements. The attached DMS contract (comprised of the Master Agreement [Exhibit 1] and Customer Guide [Exhibit 2]) and RCI contract [Exhibit 3] are taken directly from Authenticom's own preliminary injunction motion. The Data Exchange Agreement [Exhibit 4] was also tendered by both parties at the temporary injunction hearing without objection. The Court is therefore entitled to look to the text of these contracts in ruling on this Motion to Dismiss. More importantly, where the text of the contracts contradicts or does not support allegations made in the Complaint, the language of the contracts controls. *See, e.g.*, *Cousins Subs Sys., Inc. v. McKinney*, 59 F. Supp. 2d 816, 819 (E.D. Wis. 1999) ("Where the allegations of a complaint are inconsistent with the terms of a written contract attached as an exhibit, the terms of the contract prevail over the averments differing therefrom.").

C. All of Authenticom's Claims Fail Because Its Accessing of Reynolds' Systems Is Illegal

The Sherman Act is not a weapon for plaintiffs to demand from the court that which the law forbids. As set forth below, the conduct admitted by Authenticom in its own complaint

[2] Reynolds DMS contracts are referenced in paragraphs 3, 11, 67, 103, 149-150, 152, 225, 254-255; Reynolds' RCI agreements are referenced in paragraphs 11, 103, 149, 157-158, 163-165, 169, 254-255; and the Reynolds-CDK agreements are referenced in paragraphs 8, 132-138, and 243-249.

violates the federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, and numerous state statutes including Wisconsin's. This dooms all of Authenticom's claims.

"Courts have long recognized that 'an action under the antitrust laws will not lie where the business conducted by the plaintiff, and alleged to have been restrained by the defendant, was itself unlawful." *Modesto Irrigation Dist. v. Pac. Gas & Elec. Co.*, 309 F. Supp. 2d 1156, 1169-70 (N.D. Cal. 2004) (quoting *Jenkins v. Greyhound Lines, Inc.*, C-46141-RHS, 1971 WL 529, at *1 (N.D. Cal. May 4, 1971)), *aff'd*, 158 F. App'x 807 (9th Cir. 2005). In *Modesto*, an irrigation district sued because it was unlawfully being blocked by PG&E from expanding into Pittsburg, claiming that this blocking violated Sections 1 and 2 of the Sherman Act. *See id.* at 1158. But the district court concluded that the plaintiff "possessed neither the legal right nor the necessary [] permission" to conduct such activity under California statute. *Id.* at 1170. Accordingly the district court denied its claims in full, and the Ninth Circuit affirmed because plaintiff was "not a lawful competitor" of defendant. 158 F. App'x at 807.

The Seventh Circuit has reached similar conclusions. *See Maltz v. Sax*, 134 F.2d 2, 4 (7th Cir. 1943) ("Assuming as we do that the Anti-Trust Act was enacted to protect the public by preventing restraints on commerce and, generally speaking, was a public benefit measure, it still seems rather paradoxical to permit plaintiff to invoke its protection for a business, the practice of which is against public policy, if not illegal."); *see also United Airlines, Inc. v. U.S. Bank NA*, 406 F.3d 918, 924 (7th Cir. 2005) (Easterbrook, J.) (holding that no antitrust liability could attach to defendants exercising their rights under another federal statute (11 U.S.C. § 1110)). Various other cases and courts have likewise refused to allow antitrust claims for behavior that is illegal:

- No antitrust liability for restraining importation of drugs from Canada where such importation violated the FFDCA. *See In re Canadian Import Antitrust Litig.*, 470 F.3d 785, 790-92 (8th Cir. 2006);

- No antitrust liability for refusing to license technology to plaintiff for a product that "almost certainly" violated the DMCA. *See RealNetworks, Inc. v. DVD Copy Control Ass'n*, Nos. C 08-4548 MHP, C0 8-4719 MHP, 2010 WL 145098, at *6 (N.D. Cal. Jan. 8, 2010).

Courts often frame this result as a lack of viable antitrust injury: where the plaintiff's business is illegal, it cannot prove a valid injury of the sort that the antitrust laws are intended to remedy. *See, e.g.*, *Modesto*, 309 F. Supp. 2d at 1170 ("[A] party cannot prove a cognizable antitrust injury when it itself engaged in unlawful conduct *ex ante*."). Regardless of the precise reasoning, however, the result is inescapable: the claims fail.

The same result is true under the laws of tortious interference. To assert a claim for tortious interference, Authenticom must show that its contracts are valid and enforceable. *See, e.g.*, *Behnke v. Hertz Corp.*, 235 N.W.2d 690, 692 (Wis. 1975) ("While it is alleged that the Hertz Corporation maliciously induced the termination of the contract, Hertz's conduct is irrelevant if the contract itself is void as being unreasonable."). But a contract is void if it is illegal. "A contract is illegal where its formation or performance is expressly forbidden by a civil or criminal statute or where a penalty is imposed for doing the act agreed upon." *Hiltpold v. T-Shirts Plus, Inc.*, 298 N.W.2d 217, 220 (Wis. Ct. App. 1980). "And a contract in violation of a statute is void although the statute fails to provide expressly that contracts made in violation of its provisions shall not be valid." *Melchoir v. McCarty*, 31 Wis. 252, 254 (1872).[3]

[3] As the Supreme Court of Wisconsin stated in full:

> The general rule of law is, that all contracts which are repugnant to justice, or founded upon an immoral consideration, or which are against the general policy of the common law, or contrary to the provisions of any statute, are void; and that, if a party claiming a right to recover a debt is obliged to trace his title or right to the debt through any such illegal contract, he cannot recover, because he cannot

As set forth below, Authenticom's contracts that purportedly give it access to Reynolds' DMS or call for Authenticom to perform such access are illegal and void—as a matter of law—under the CFAA, the WCCA, and multiple other statutes and bodies of law. Authenticom's claims for interference with those contracts should therefore be dismissed. *See, e.g.*, *Stamatiou v. U.S. Gypsum Co.*, 400 F. Supp. 431, 435 (N.D. Ill. 1975), *aff'd*, 534 F.2d 330 (7th Cir. 1976) ("Since the agreement is unenforceable, there could be no malicious interference with rights created by it."); *see also* RESTATEMENT (SECOND) OF TORTS § 774 ("One who by appropriate means causes the nonperformance of an illegal agreement or an agreement having a purpose or effect in violation of an established public policy is not liable for pecuniary harm resulting from the nonperformance.").

D. Authenticom's Actions, Contracts, and Requested Relief Are All Illegal

A fundamental premise of the CFAA is that accessing a computer without proper authorization is illegal. As set forth below, Authenticom's own pleaded facts admit that it has violated the CFAA. More importantly for purposes of the present Motion, Authenticom's pleaded claims run squarely afoul of the CFAA, asking the Court to order access to Reynolds' computer systems that would, in any other universe, be unauthorized and illegal. The same is true under numerous other statutes and bodies of law as well. As set forth below, that illegality

---

> be allowed to prove the illegal contract as the foundation for his right of recovery. It is quite immaterial whether such illegal contract be *malum in se*, or only *malum prohibitum*. In either case the maxim, *ex turpi causa non oritur actio*, is applicable. And a contract in violation of a statute is void although the statute fails to provide expressly that contracts made in violation of its provisions shall not be valid. It is sufficient that it is prohibited, and its invalidity follows as a legal consequence.

Melchoir v. McCarty, 31 Wis. 252, 254 (1872).

is inescapable on the face of Authenticom's Complaint. That illegality dictates the dismissal of Authenticom's claims.

1. Authenticom's Accessing of Reynolds' DMSs Falls Squarely Within the CFAA's Prohibitions

Per the CFAA's plain text, anyone who intentionally accesses a computer without its owner's authorization and thereby obtains information violates the statute. *See* 18 U.S.C. § 1030(a)(2)(C). Similarly, anyone who intentionally accesses a computer without its owner's authorization and causes damage and loss violates the statute. *See* 18 U.S.C. § 1030(a)(5)(C). Authorization is also not binary: a party can be authorized only to access the system in limited and specific ways, and if that authorization is exceeded the statute is violated. *See id.*; *see also Musacchio v. United States*, 136 S. Ct. 709, 713 (2016) ("The statute thus provides two ways of committing the crime of improperly accessing a protected computer: (1) obtaining access without authorization; and (2) obtaining access with authorization but then using that access improperly."). The CFAA is primarily a criminal statute, but it also provides private rights of action for parties who suffer damage or loss above a certain threshold as a result of a CFAA violation. *See Farmers Ins. Exch. v. Auto Club Grp.*, 823 F. Supp. 2d 847, 852 (N.D. Ill. 2011) ("Although the CFAA is generally criminal in nature, it also provides a private right of action for a person 'who suffers damage or loss by reason of a [CFAA] violation.'" (quoting 18 U.S.C. § 1030(g))).

The specific statutory language at issue states: "[w]hoever … intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains … information from any protected computer," is subject both to criminal and civil liability. 18 U.S.C. § 1030(a)(2)(C); *see also id.* § 1030(c) (criminal penalties); *id.* § 1030(g) (civil damages and injunctive relief). Each of these elements is readily satisfied under Authenticom's pleaded facts.

First, Reynolds' DMS is both a "computer" and a "protected computer" under the CFAA. A "computer" is defined as computing devices themselves, as well as "*any data storage facility or communications facility* directly related to or operating in conjunction with such device." *Id.* § 1030(e)(1) (emphasis added); *see also, e.g., United States v. Nosal*, 844 F.3d 1024, 1032 n.2 (9th Cir. 2016) (citing cases applying the CFAA to "computer networks" and "databases").[4] And a computer is "protected" so long as it "used in or affecting interstate or foreign commerce or communication." *Id.* § 1030(e)(2)(B). Authenticom's pleaded facts readily establish that Reynolds' DMS systems are "protected computers." *See, e.g.*, Compl. ¶¶ 3, 29.

The next element is whether Authenticom intentionally accessed Reynolds' DMS and obtained information. *See* 18 U.S.C. § 1030(a)(2)(C). This too is pleaded—Authenticom explicitly pleads that it uses dealer-provided login credentials to "access the DMS database to pull the data." Compl. ¶ 55. Indeed, accessing DMS databases to obtain information is Authenticom's primary business model. *See id.* ¶¶ 55, 77, 79. Authenticom further admits that it engaged in various workarounds and strategies to circumvent Reynolds' system security measures. *See id.* ¶¶ 195, 197, 199.

The final element is whether Authenticom's accessing of Reynolds' DMSs is "without authorization" or "exceeds authorization." As the Complaint itself makes clear, Authenticom does not have Reynolds' authorization to access Reynolds' proprietary systems. According to

[4] *See also LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1136 (9th Cir. 2009) (website storing data was "protected computer"); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581 (1st Cir. 2001) (use of "scraper" to remove data from travel website constituted unauthorized access to "protected computer"); *Estes Forwarding Worldwide LLC v. Cuellar*, No. 3:16-CV-853-HEH, 2017 WL 931617, at **2, 7 (E.D. Va. Mar. 9, 2017) (Google Drive account used to record shipments, routing, vendors, and cost information was a "protected computer" under CFAA); *Cont'l Grp., Inc. v . KW Prop. Mgmt., LLC*, 622 F. Supp. 2d 1357, 1370 (S.D. Fla. 2009) (property management company's "computer system" was a "protected computer" under CFAA).

Authenticom, Reynolds has denied that authorization to Authenticom since 2007 and has been actively implementing technological measures to block and prevent such access for the past decade. *See* Compl. ¶¶ 6, 92, 189. Authenticom further admits that Reynolds' contracts bar dealers from giving third parties access to the DMS—as the contract itself makes very explicit. *See* Ex. 1 § 1; Ex. 2 at 19-22; Compl. ¶¶ 11, 103, 149-150, 152-153.

Indeed, Reynolds' standard DMS contract (unremarkably) is a limited license agreement containing certain exclusions, one of which is that there will be no use of access by third parties. In this regard, the agreement states:

> Reynolds (or Other Providers) retains all proprietary rights in the Licensed Matter and the Site, Including copyrights, patents and trade secrets. You acknowledge that Licensed Matter [*e.g.*, the DMS] contains Confidential Information belonging to Reynolds or Other Providers and that Licensed Matter may be subject to end user license agreements of Other Providers. **You agree**: (a) not to copy (other than making regular back-up copies, if permitted by us), modify, disassemble or decompile any Licensed Matter or the Site, **or re-license, sublicense, rent, lease, timeshare or act as a service bureau**; (b) **to maintain the Licensed Matter in complete confidence**; (c) **not to disclose or provide access to any Licensed Matter or non-public portions of the Site to any third party, except your employees who have a need for access to operate your business and who agree to comply with your obligations under this Section 1**; (d) **to notify Reynolds immediately of any unauthorized Use or disclosure of Licensed Matter or your PIN or Logins** (if applicable); (e) **to cooperate with us to protect Reynolds and Other Providers' proprietary rights in Licensed Matter and the Site**, and (f) to comply with any end user license agreement of an Other Provider. ...

Ex. 1 § 1. Therefore, when Authenticom contends that it has permission from dealerships to use the DMS, that is a red herring. A dealer cannot give a right to a third party that it does not possess (as affirmed by multiple cases below).

Reynolds also took the public position that its DMS contracts forbade unauthorized third party access—and that attempts to gain such access violated the CFAA—in a lawsuit that Reynolds filed against Superior Integrated Solutions ("SIS") in the United States District Court

for the Southern District of Ohio in 2012.[5] Finally, Authenticom admits in its own pleading that Reynolds had informed it that its efforts to access Reynolds' systems were unauthorized in an April 6, 2015 cease-and-desist letter. *See* Compl. ¶ 156.

Thus, Authenticom's own pleaded facts establish that its business model, with respect to Reynolds' proprietary systems, is one that is illegal under the CFAA.[6]

2. Authenticom's Actions, Contracts, and Remedies Are Illegal Under Numerous Other Statutes and Bodies of Law as Well

The Wisconsin Computer Crimes Act ("WCCA"), WIS. STAT. § 943.70, similarly outlaws Authenticom's accessing of Reynolds' DMS, except that the analysis is even simpler than under the CFAA. Like its federal counterpart, the Wisconsin statute broadly defines "computer" to include not just computing devices themselves, but also "all input, output, processing, storage, computer software and communication facilities that are connected or related to a computer in a computer system or computer network." *Id.* § 943.70(1)(am). In addition, the WCCA "makes it unlawful to 'willfully, knowingly and without authorization' (1) access, take possession of, or copy 'computer programs or supporting documentation'; or (2) disclose 'restricted access codes or other restricted access information to unauthorized persons.'" *Epic Sys. Corp. v. Tata Consultancy Servs. Ltd.*, No. 14-cv-748-wmc, 2016 WL

[5] *See generally The Reynolds & Reynolds Co. v. Superior Integrated Solutions, Inc.*, case no. 1:12-cv-00848 (S.D. Ohio). Authenticom references this lawsuit in its Complaint and it is thus properly considered. *See* Compl. ¶ 107; *Hecker*, 556 F.3d at 582. Authenticom fails to explicitly note the CFAA claim, but the Court may take judicial notice of the fact that Reynolds' complaint against SIS pleaded such a claim. *See Henson v. CSC Credit Servs.*, 29 F.3d 280, 284 (7th Cir. 1994). A copy of Reynolds' Original Complaint in that case is attached as Exhibit 5 [hereinafter "SIS Compl."].

[6] Reynolds' ability to bring affirmative, civil claims for those violation requires a showing of additional elements—namely, damage or loss in excess of $5,000 in a single year—but that element determines only whether Reynolds has a civil remedy, not whether Authenticom's actions are illegal. Reynolds will demonstrate this element in connection with its counterclaims.

4033276, at *23 (W.D. Wis. July 27, 2016). Here again, Authenticom's own Complaint demonstrates that it has undertaken all of these illegal acts. *See* Compl. ¶¶ 6, 92, 189.

Other bodies of law similarly uphold the validity of Reynolds' right to control system access and the impropriety or illegality of Authenticom's efforts to undermine or breach that control. For example, California's computer crime statute states that any person who "knowingly and without permission uses or causes to be used computer services" is guilty of a public offence. CAL. PENAL CODE § 502(c). "Computer services" is defined to include "computer time, data processing, or storage functions, Internet services, electronic mail services, electronic message services, or other uses of a computer, computer system, or computer network"—which readily encompasses Authenticom's unauthorized use and accessing of Reynolds' DMS. *Id.* § 502(b)(4). "For purposes of Section 502, parties act without permission when they circumvent technical or code-based barriers in place to restrict or bar a user's access." *Satmodo, LLC v. Whenever Commc'ns, LLC*, 17-CV-0192-AJB NLS, 2017 WL 1365839, at *6 (S.D. Cal. Apr. 14, 2017) (marks omitted). Authenticom's actions, contracts and remedies are thus clearly illegal under California law as well.[7]

Similarly, numerous courts have held that unauthorized data scraping can constitute trespass to chattels. *See, e.g.*, *Register.Com, Inc. v. Verio*, 356 F.3d 393, 404-05 (2d Cir. 2004) (upholding district court preliminary injunction for trespass to chattels against data scraper that "access[ed] Register's computers by automated software programs performing multiple successive queries"); *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1027 (S.D. Ohio. 1997) ("Defendants' intentional use of plaintiff's proprietary computer equipment exceeds plaintiff's consent and, indeed, continued after repeated demands that defendants cease. Such use

[7] Other states have similar statutes that equally and variously condemn Authenticom's behavior, which cumulatively illustrates its illegality.

is an actionable trespass to plaintiff's chattel."). As highlighted by the Second Circuit, the harm flowed not only from the specific scraper at issue, but also from the fact that allowing one party to engage in such scraping would encourage others to do so. *See* 356 F.3d at 404 ("While Verio's robots alone would not incapacitate Register's systems, the court found that if Verio were permitted to continue to access Register's computers through such robots, it was 'highly probable' that other Internet service providers would devise similar programs to access Register's data, and that the system would be overtaxed and would crash."). Just so here: the problem is not merely Authenticom's access, it is all the others who will demand that same DMS access for themselves. Utilizing another's property without compensation—as Authenticom admittedly does with respect to Reynolds' DMS—constitutes unjust enrichment as well. *See, e.g.*, *Oce N. Am., Inc. v. MCS Servs., Inc.*, 748 F. Supp. 2d 481 (D. Md. 2010).

For all of these reasons, Authenticom—and everyone else—is legally forbidden to access Reynolds' DMS without Reynolds' authorization and permission.

3. Authenticom Has No Valid Defense of Its Illegal Actions and Contracts

Authenticom's primary expected defense to the CFAA and other charges of illegality is that the dealers gave Authenticom permission to access Reynolds' system on their behalf. But that entirely begs the question whether the Authenticom contracts granting such permission were illegal in the first place. Moreover, numerous cases, including the Ninth Circuit's recent *Facebook* opinion, emphatically reject Authenticom's position that such licensed user permission excuses the violation. *See Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016), *pet. for cert. pending in* No. 16-1105.

As here, the defendant in *Facebook* argued that it had received permission from its users to access their social media accounts and gather information. As here, the defendant performed

that information gathering using login credentials provided by those users. As here, the owner of the database where that information was stored—Facebook—objected to and sought to block that access. As here, Facebook sent an explicit cease-and-desist letter stating that the access was unauthorized. And as here, the defendant used various workarounds to circumvent that blocking and continued its efforts despite Facebook's explicit demands. When the defendant (Power) refused, Facebook sued.

Like Authenticom, Power asserted that its conduct did not violate the CFAA because it had been authorized by its customers, the users, to access their accounts and data. The district court rejected this position and granted summary judgment to Facebook as a matter of law. The Ninth Circuit affirmed and emphatically rejected Power's argument that its use of Facebook was somehow "authorized" because some Facebook *users* had provided their login credentials to Power. "The consent that Power had received from Facebook users was not sufficient to grant continuing authorization to access Facebook's computers after Facebook's express revocation of permission." *Id.* at 1068. The court offered "[a]n analogy from the physical world [that] may help to illustrate why this is so":

> Suppose that a person wants to borrow a friend's jewelry that is held in a safe deposit box at a bank. The friend gives permission for the person to access the safe deposit box and lends him a key. Upon receiving the key, though, the person decides to visit the bank while carrying a shotgun. The bank ejects the person from its premises and bans his reentry. The gun-toting jewelry borrower could not then reenter the bank, claiming that access to the safe deposit box gave him authority to stride about the bank's property while armed. In other words, to access the safe deposit box, the person needs permission *both* from his friend (who controls access to the safe) *and* from the bank (which controls access to its premises).

Id. This analogy that applies with equal force to Authenticom's claim.

> Similarly, for Power to continue its campaign using Facebook's computers, it needed authorization both from individual Facebook users (who controlled their data and personal pages) and from Facebook (which stored this data on its

> physical servers). ***Permission from the users alone was not sufficient to constitute authorization after Facebook issued the cease and desist letter***.

Id. (emphasis added). Facebook had "plainly put Power on notice that it was no longer authorized to access Facebook's computers." *Id.* at 1067 n.3. And "[o]nce permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability" under the CFAA. *Id.* at 1067.

Under the specific requirements outlined by the Ninth Circuit, Authenticom's contracts are plainly illegal. Just like Facebook, Reynolds has made clear to Authenticom on numerous occasions that it was not authorized or permitted to access Reynolds' DMS. Moreover, the facts here demonstrate illegality even more clearly. Much of the Ninth Circuit's emphasis on Facebook's explicit revocation of permission stemmed from the fact that Facebook is a publicly accessible website, and the court went to great lengths to clarify that its holding of illegality did not extend to the "permission skirmishes that ordinary Internet users may face." *Id.* at 1069. This case present no such concerns: the Reynolds DMS is not a website, is not publicly accessible, and is not governed by mere website terms of use. Further the *consumer* data stored on the DMS is not information shared by users with all of their "friends." There is no allegation that Authenticom has *any* permission from the *consumers* (car buyers and service customers) whose data it is selling and distributing.

Other decisions support this result. One district court recently granted an injunction *against* a party that, while authorized to access a physical computer by its owner, was illegally accessing proprietary software on that computer without authorization of the software's owner. *See Philips Med. Sys. Puerto Rico Inc. v. GIS Partners Corp.*, 203 F. Supp. 3d 221, 235 (D.P.R. 2016) ("Put another way, while defendants likely had some authority to access the computer (which they obtained from Medical X-Ray and the Hospital), they likely exceeded that authority

by hacking into proprietary software—the CSIP Tool (where Phillips maintains proprietary data and files)—without any authorization whatsoever from Phillips."). Here, Authenticom has done the same and more. Under that court's reasoning, it is Authenticom that should be enjoined—rather than the other way around.[8]

Another court, in the Northern District of Ohio, squarely held that the CFAA prohibits hostilely accessing a database to extract customer information with the customer's—but not the database owner's—permission. *See Snap-on Bus. Solutions, Inc. v. O'Neil & Assocs., Inc.*, 708 F. Supp. 2d 669 (N.D. Ohio 2010). There, Snap-on provided customers with a searchable database of automotive and heavy-equipment parts, with the parts information being supplied by the customers (primarily in the form of parts catalogues). *See id.* at 672. One Snap-on customer, Mitsubishi, decided that it wanted to move its business to a different platform. In conjunction with that decision, Mitsubishi authorized its new provider (Defendant O'Neil) to use

---

[8] A recent Nevada federal case under California's computer statute recently rejected Authenticom's core thesis as well:

> As to defendants' second argument, defendants argue that the testimony and documents at trial established that Rimini was specifically authorized by its clients (who had software licenses for Oracle software) to access Oracle America's website. Defendants contend that it is undisputed that they had permission from their clients to access the website in order to download support materials for those clients and that defendants did not exceed the scope of that authorization. . . .
>
> Defendants' argument is without merit.

Oracle USA, Inc. v. Rimini St., Inc., 191 F. Supp. 3d 1134, 1143 (D. Nev. 2016). The court relied in large part on the fact that the defendants used automated tools to access the website—which was prohibited by the website terms of use—and did so despite Oracle's efforts to block the tools in question. *See id.* at 1144-45. As the court encapsulated: **"[D]efendants' entire argument boils down to the nonsensical assertion that their clients granted them the right to do something the clients themselves did not have the right to do, namely, log on to Oracle America's website and take material from the website with prohibited automated tools.** This argument is completely untenable." *Id.* (emphasis added).

Mitsubishi's logins to run a data-scraping program on Snap-on's database to pull Mitsubishi's data out. *See id.* at 674. This assertedly caused Snap-on's website to crash, and Snap-on blocked O'Neil's IP address. *See id.* at 675. O'Neil worked around this block and continued scraping the data for a time, until Snap-on reinstituted the block and sued. *See id.*

Snap-on claimed O'Neil had violated the CFAA, among other things. O'Neil claimed in defense that it had been authorized by Mitsubishi to access the website and pull the data. The court refused to grant summary judgment to O'Neil, holding that the question ultimately turned on whether Mitsubishi's license agreement with Snap-on permitted Mitsubishi to authorize such access. *See id.* at 678. In *Snap-on*, that aspect of the license agreements was a disputed question of fact. Here, on the other hand, it is literally admitted and alleged in Authenticom's complaint that Reynolds' DMS license agreements do **not** allow dealers to authorize such access. *See, e.g.*, Compl. ¶¶ 11, 149-150, 152, 254-255. Under the *Snap-on* court's reasoning as well, Authenticom is in violation of the CFAA as a matter of law.[9]

Other cases similarly affirm that the use of unauthorized login credentials to obtain information is illegal. In *State Analysis*, the Eastern District of Virginia held that a defendant "may not hide behind purported 'authorization'" given to it by a licensee when the defendant knew that the terms of the license stated that only the licensee-client itself was authorized to use the services in question. *See State Analysis, Inc. v. Am. Fin. Servs. Assoc.*, 621 F. Supp. 2d 309, 316 (E.D. Va. 2009). In the recent *Epic Systems* case, this Court held that a clear violation of the CFAA had occurred where a contractor used login credentials from a former employee to access the Epic Systems UserWeb (as well as "the server which houses it") to obtain information. *See*

[9] The *Snap-on* court also denied summary judgment to O'Neil on Snap-on's claim for trespass to chattels, holding that liability could readily attach to such behavior under that theory as well. *See id.* at 679-80. Again, this all supports the clear illegality of Authenticom's actions and requested relief.

Epic Sys. Corp. v. Tata Consultancy Servs. Ltd., No. 14-cv-748-wmc, 2016 WL 4033276, at *23 (W.D. Wis. Jul. 27, 2016) (post-trial motions pending). And in *Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178 (N.D. Cal. 2013), the court held that a data "scraper's" access was "unauthorized" under the CFAA given its "persistent scraping efforts undertaken after (1) receiving a cease-and-desist letter and (2) employing IT rotation technology to mask its identity and overcome Craigslist's technological barriers." *Id.* at 1187.

Although CFAA cases sometimes present complicated questions around authorization, access, and intent, this case presents no such obstacles. This is not a situation involving innocent Internet users violating a shrink-wrapped license at the bottom of a web page, or an employee accidentally exceeding the scope of his employer-permitted use. Reynolds' DMS is a closed, proprietary enterprise platform that is licensed only to business entities pursuant to specifically negotiated contracts. Authenticom does not dispute this. Authenticom flaunts the fact that it has accessed Reynolds' DMS, despite unequivocal knowledge that such access was not authorized by Reynolds, using a variety of devious technical workarounds.

The contracts Authenticom claims give it the right and/or obligation to engage in this behavior are thus illegal and void. Reynolds' efforts to defend its own systems are not tortious interference, nor are they antitrust violations. In short, Authenticom's claims must be dismissed because of this fundamental illegality.

4. *WIREdata* Does Not Alter the Analysis

In past briefing, Authenticom relies on a copyright case from the Seventh Circuit as support for its position that it can legitimately access Reynolds' DMS. *See Assessment Tech. of WI, LLC v. WIREdata, Inc.*, 350 F.3d 640 (7th Cir. 2003). But *WIREdata* was exclusively a Copyright Act case and did not involve claims under the CFAA, the WCAA, or Wisconsin contract and tort law. *See id.* at 641. As the Court explained, the case was "about the attempt of

a copyright owner to use copyright law to block access to data that not only are neither copyrightable nor copyrighted, but were not created or obtained by the copyright owner." The Seventh Circuit held that the doctrine of copyright did not provide such a claim. In doing so, the court found that the plaintiff was not suing for tortious interference with its licensing agreements, which "would be the logical route for complaining about WIREdata's inviting the municipalities that are AT's licensees to violate the terms of their licenses." *Id.* at 646. The court further acknowledged that there are "contractual solutions to the problem of copying the contents of databases"—the extent of which were apparently "ambiguous" in AT's own contracts, and not part of any actual claims in the case. *See id.* The case is readily distinguishable on numerous other grounds as well, including the fact that the case involved open-records data (the openness of which was required under state law), and the plaintiff's position that any data exported to third parties was a violation of its copyright. Here, the opposite is true: the privacy of the data is required, and Reynolds has no problem with dealers exporting and sending data to third parties, so long as they do not access the DMS directly. And again, the case involved no claims under the CFAA or any other statute for illegal computer access or related activities. The Court should therefore apply the plain text of the CFAA and hold Authenticom's contracts, actions, and requested relief to be illegal.

E. Authenticom Fails to Allege Plausible Antitrust Causes of Action

Even if the claims are not dismissed, as they must be, because Authenticom has pleaded this case is in aid of its illegal activity, the Complaint still must be dismissed for failure to state a claim. Authenticom's claims suffer from fatal pleading deficiencies under the antitrust laws themselves. Reynolds recognizes that the Court preliminarily determined in the preliminary injunction context that Authenticom establishes at least a moderate chance of success in proving that the defendants have violated the Sherman Act. In light of the highly compressed nature of

that review and subsequent limited analysis of the antitrust laws, however, Reynolds respectfully urges the Court to review the arguments and authorities set forth below. In sum, Authenticom fails to state a plausible claim for relief under its horizontal, vertical, or unilateral antitrust theories.

1. Authenticom Fails to State a Horizontal Conspiracy Claim (First Cause of Action)

Authenticom's marquee claim is its theory that Reynolds and CDK entered into a horizontal agreement, codified into writing, to eliminate competition in the dealer data integration market and their respective aftermarkets by: (1) participating in a "market division" arrangement where each Defendant agreed to no longer compete in the dealer data integration market; and (2) engaging in a "group boycott" to block all hostile data integrators and other third parties from accessing dealer data stored on Defendants' respective DMS platforms. Compl. ¶¶ 7-8, 245. As set forth below, this claim fails on multiple, dispositive legal grounds.

i. The February 2015 Agreements do not establish or support the alleged conspiracy

The core of Authenticom's horizontal conspiracy case is an alleged "per se illegal written agreement . . . categorized as a 'Wind Down Access Agreement.'" Compl. ¶ 132. Authenticom claims to quote the agreement's "key provision" to state that "CDK 'covenants and agrees not to integrate with, access, or attempt to integrate with or access, any Reynolds-brand DMS – either CDK itself or through any current or future affiliated subsidiary,' which includes CDK subsidiaries Digital Motorworks and IntegraLink." Compl. ¶ 134. ***But the agreement does not say this at all. See*** Ex. 4. As shown by the actual agreement (the "DEA"), which the Court can consider for purposes of this motion to dismiss, the alleged "key" provision showing a horizontal conspiracy literally does not exist.

Nor is there anything in the DEA that supports Authenticom's theories of "market division" or "group boycott." The DEA makes no reference to Authenticom, to CDK's DMS, or to what either company will do with respect to data integration more broadly. After Authenticom was provided with the DEA, it pivoted to section 4.5 as the basis for its conspiracy allegations, but that unpleaded provision merely requires both parties to (1) not share intellectual property, know-how, and other materials learned during the course of the wind-down with affiliates or other third parties and (2) not assist others in hostilely accessing their respective DMSs. It is not anticompetitive to restrict use of confidential information in this manner. *See, e.g.*, *IDX Systems Corp. v. Epic Sys. Corp.*, 285 F.3d 581, 585 (7th Cir. 2002) ("[N]othing in the antitrust laws gives one producer a right to sponge off another's intellectual property").

At most, the DEA indicates that CDK intended to cease accessing Reynolds' DMS without authorization. But that is not an illegal, anticompetitive horizontal conspiracy. To start, the agreement is not horizontal from an economic perspective. To be a horizontal agreement, the participants must be "(1) actual or potential rivals at the time the agreement is made; and (2) the agreement eliminates some avenue of rivalry among them." P. Areeda & H. Hovenkamp, ANTITRUST LAW ¶ 1901b (3d ed. 2006) (hereinafter "Areeda & Hovenkamp"). The mere fact that the contracting parties — Reynolds and CDK — are horizontal competitors with respect to their DMS products does not mean that all of their agreements are horizontal. Here, the DEA did not eliminate any rivalry between Reynolds and CDK: the only thing it did was unwind CDK's illegal accessing of Reynolds' DMS. That was not a rivalry—it was trespass. And at the time of the DEA, Reynolds was already successfully blocking CDK's own data-integration from accessing Reynolds' system anyway. *See* Compl. ¶ 92.

But even assuming the DEA were horizontal, that still would not render it illegal: it must also be anticompetitive. *See, e.g.,* Areeda & Hovenkamp ¶ 1901b ("Simply to conclude that an agreement is horizontal establishes nothing about whether it is competitive or anticompetitive."). Far from being anticompetitive, the DEA (or "wind down" agreement) is a perfectly lawful resolution to a legal dispute: specifically, the aftermath of Reynolds sending cease-and-desist letters to CDK under the CFAA and successfully blocking CDK from hacking into Reynolds' DMS platforms. CDK's efforts to access Reynolds' DMS without authorization were illegal just like Authenticom's. Unwinding that unauthorized access in a manner designed to safely reduce dealer business disruption is not anticompetitive, nor is it unreasonable. *See Texaco Inc. v. Dagher*, 547 U.S. 1, 5 (2006) (holding that Section 1 prohibits only "unreasonable" restraints).

In sum, nothing in the alleged 2015 agreement states that CDK and Reynolds have agreed to an illegal or unlawful agreement in restraint of trade. Moreover, the agreement does not even establish the far-more-limited premise that Reynolds and CDK agreed to block Authenticom or any other third party from having system access to their respective DMS platforms. Given the centrality of the DEA to Authenticom's complaint, this claim should be dismissed on this basis alone.

ii. Authenticom's allegations of a "confessed" conspiracy agreement fail as well

Beyond the written agreements, what remains is Authenticom's bald allegation that Reynolds and CDK both confessed to a conspiracy, in separate conversations over a year apart. As an initial matter, the most plausible interpretation of those alleged "confessions" is that they simply referred to the DEA, which as established above is not illegal at all. But Authenticom characterizes its conspiracy allegation in various other ways as well, alleging either that (a)

Reynolds and CDK mutually agreed to stop hostilely accessing each other's systems, or (b) Reynolds and CDK mutually agreed to maintain their DMSs as closed systems.

The former theory fails on its face. Since 1911, the Supreme Court has held that Section 1 prohibits only "unreasonable" restraints of trade, *Standard Oil Co. v. United States*, 221 U.S. 1, 60-68 (1911); *see also Texaco*, 547 U.S. at 5, and it cannot be an "unreasonable" restraint for purposes of an antitrust conspiracy to agree to follow the law. And yet that is precisely what Authenticom has alleged here: that Reynolds and CDK "conspired" to cease violating the CFAA (and other laws) with respect to each other's systems. That is no more illegal than two competitors agreeing to both pay their taxes, adhere to applicable industry regulations, or abide by the Foreign Corrupt Practices Act. Federal law, and the Sherman Act, should be read to promote such agreements, not to outlaw them. *See Bd. of Trade of City of Chicago v. United States*, 246 U.S. 231, 238 (1918) ("The history of the restraint, the evil believed to exist, the reason for adopting the particular remedy, the purpose or end sought to be attained, are all relevant facts.").

Furthermore, all of these broader conspiracy allegations are implausible under Authenticom's own pleaded facts. As noted above, the seminal case of *Bell Atlantic Corp. v. Twombly* provides that antitrust conspiracy allegations do not pass through the motion-to-dismiss gate unless they are ***more plausible*** than explanations for independent but parallel marketplace behavior. 550 U.S. at 545-46. When allegations of parallel conduct are set out in order to make a Section One claim, "they must be placed in a context that raises a suggestion of a preceding agreement, not merely parallel conduct that could just as well be independent action." *Id.* at 557. Indeed, the Supreme Court "has never held that proof of parallel business behavior conclusively

establishes agreement or, phrased differently, that such behavior itself constitutes a Sherman Act offense." *Theatre Enters., Inc. v. Paramount Film Distrib. Corp.*, 346 U.S. 537, 540 (1954).

But in this case, Authenticom affirmatively alleges that Reynolds and CDK's conduct was ***not even parallel***—most importantly with regard to the timing of their respective decisions to (1) close their respective DMS systems to outside parties and (2) not to engage in illegally accessing other providers' DMSs without authorization. As admitted in the Complaint, CDK reached these decisions in 2015; but Reynolds closed its system no later than ***2007***, and Reynolds ***never*** engaged in the business of hostile integration. *See* Compl. ¶¶ 6, 102 & n.24. As the Ninth Circuit recently held, "[a]llegations of such slow adoption of similar policies does not raise the specter of collusion." *In re Musical Instruments & Equip. Antitrust Litig.*, 798 F.3d 1186, 1195–96 (9th Cir. 2015). Reynolds is unaware of any antitrust case suggesting that a conspiracy can be alleged based on actions that occurred in different decades.

The plausibility of Authenticom's allegations is further belied by the lack of any interdependency. Simply put, Reynolds did not need CDK's agreement to move to a closed system; Reynolds had already unilaterally implemented such a system for over a decade. *See* Compl. ¶¶ 6, 74, 92, 107-109. Likewise, CDK's decision to move to a more closed enterprise software architecture did not require any agreement from Reynolds. CDK already knew Reynolds' policies, and Authenticom's own allegations about the emphatic nature of Reynolds' policies—in combination with Reynolds' 2012 SIS lawsuit declaring hostile integration to be illegal, *see* Ex. 5—make clear that it is not plausible that Reynolds would ever change course.

In sum, there is simply no plausible reason alleged for a conspiracy — neither Reynolds nor CDK needed the other to agree to any of their conduct, at any point. As a matter of well-established antitrust law, when firms have "no rational economic motive to conspire, and if their

conduct is consistent with other, equally plausible explanations, the conduct does not give rise to an inference of conspiracy." *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 596-97 (1986); *see also Miles Distrib., Inc. v. Specialty Constr. Brands, Inc.*, 476 F.3d 442, 452 (7th Cir. 2007). Furthermore, "[t]he mere existence of mutual economic advantage, by itself, does not tend to exclude the possibility of independent, legitimate action and supplies no basis for inferring a conspiracy." *Serfecz v. Jewel Food Stores*, 67 F.3d 591, 600-01 (7th Cir. 1995) (internal citations omitted). At most, Authenticom's allegations show that CDK adopted policies similar to Reynolds. But it is perfectly reasonably for CDK to have independently reached the same conclusions regarding system security and performance that Reynolds reached a decade earlier without a horizontal agreement to do so. In any event, for its part, ***Reynolds*** had no rational reason to so conspire, and Authenticom alleges none.

iii. Authenticom fails to allege a plausible "boycott" or "market division" agreement

To push its conspiracy allegations into the *per se* category, Authenticom attempts to characterize all of its conspiracy allegations as either a "market allocation" and/or "group boycott" agreement. But this too fails as a matter of both plausibility and legal definition.

Boiled down, Authenticom's "market division" theory is that CDK agreed to cease any attempts to provide "integration services" on Reynolds' DMS. Compl. ¶ 132. But as established above, any such attempts would have been (and were) illegal under the CFAA. And as discussed below, the Supreme Court's decision in *Trinko* affirms that Reynolds was free to make that choice. Reynolds' lawful exclusion of CDK from its DMS was therefore not a "market division." And Authenticom does not allege that the conspiracy divided the alleged market in any other way. Indeed, as Authenticom admits, Reynolds has never been a participant in the data integration "market" for non-Reynolds DMSs (*see* Compl. ¶ 102 n.24), which would preclude

any claim based on those DMSs. *See, e.g.*, *California ex rel. Harris v. Safeway, Inc.*, 651 F.3d 1118, 1137 (9th Cir. 2011) (illegal "market-allocation agreements" are "among competitors at the same market level"). It is also implausible that Reynolds would enter an agreement to "divide" a "market" in which it did not participate—and which it had stated in a publicly filed lawsuit was illegal in 2012. *See generally* Ex. 5 (SIS Compl.). This theory therefore fails.

Likewise, there can be no group boycott because there is no "refusal" to deal. A group boycott occurs when "firms with market power boycott suppliers or customers in order to discourage them from doing business with a competitor." *FTC v. Ind. Fed'n of Dentists*, 476 U.S. 447, 458 (1986). But Authenticom is neither a supplier nor a customer with respect to Reynolds' and CDK's DMSs. It has never offered to buy or sell anything from Reynolds with respect to Reynolds' DMS. Instead, Authenticom gets login credentials from dealers and is paid by vendors for its integration services. *See* Compl. ¶¶ 59-60. For purposes of hostile integration, Authenticom does not "deal" and has never "dealt" with Reynolds for data integration services on a Reynolds DMS. It cannot be a boycott to refuse to let someone trespass or use your product for free. Thus, the entire concept of a "boycott" is inapplicable here.

Moreover, the distinction between "system access" and "data access" may be subtle to an outsider, but is critical, for purposes of Authenticom's "group boycott" claims. Authenticom's allegations claim to not relate to "system access" but "data access." *Id.* ¶ 245 (alleging that the conspiracy prevents Authenticom "from *accessing data* of dealers using Defendants' respective DMS systems") (emphasis added)). But the Complaint acknowledges that Authenticom still can access dealer data through dynamic reporting and other tools. *See* Compl. ¶ 105. Authenticom's complaint does not point to any agreement that states that Reynolds and CDK would boycott or cease doing business with Authenticom. On the contrary, Authenticom explicitly pleads that

Reynolds is still using Authenticom to pull data from other DMS providers—specifically, those who have authorized Authenticom to perform such activities. *See id.* ¶ 207.[10] As Authenticom itself admits, "Reynolds is actually one of Authenticom's larger vendor clients." *Id.* In other words, Authenticom's alleged data boycott does not exist, per its own allegations.

Last but not least, it warrants emphasis that Authenticom's own requested relief betrays the notion that this is a true horizontal, *per se* conspiracy. For truly unlawful *per se* agreements, the relief is simple: void the agreement and let the market take its course. *See, e.g.*, Areeda & Hovenkamp ¶ 1903b ("In [horizontal output-limiting] cases effective judicial intervention may consist of little more than enjoining the anticompetitive agreement and permitting market forces to do their work."). There is never any need to force firms to do business with each other or with an excluded rival—which, as set forth below, virtually all modern antitrust authorities agree is an inappropriate exercise for courts to engage in. The fact that Authenticom has to ask this Court to order Reynolds and CDK to open up their systems and do "business" with it (or more accurately, allow free trespass) establishes that there is no true horizontal, *per se* conspiracy here at all.

2. Authenticom Fails to State a Claim Based on Unilateral Conduct (Fourth Cause of Action for Monopoly)

Turning now to Authenticom's claims based on unilateral conduct, Authenticom alleges that Reynolds monopolized the brand-specific dealer data integration "aftermarket" for its DMS. *See* Compl. ¶ 271. As a matter of law, Authenticom's allegations are not sufficient to state a claim under Section 2 of the Sherman Act for at least three reasons.

[10] If and when those providers rescind such authorization from Authenticom, Reynolds will cease using Authenticom for those DMSs as well—for the same simple and obvious reason that failing to do so would be illegal under the CFAA and other laws. That decision would not create any antitrust liability. Nor does the alleged agreement.

First, the Supreme Court's decision in *Trinko* and its progeny hold that a firm—even a monopolist—is not required to provide competitors or other third parties with access to its proprietary systems, period, for any reason or no reason at all. Second, the CFAA allows companies to use blocking and other similar means to protect their proprietary computer systems from trespass. Finally, Authenticom does not state a plausible "aftermarket" theory because it fails to make the necessary allegations required under the Supreme Court's rarely applied and limited decision in *Kodak*. Each of these grounds warrants dismissal of Authenticom's fourth cause of action.

i. There is no right of access under Sherman Act Section Two

The core premise of Authenticom's monopoly claim—and indeed all of its antitrust claims—is that Reynolds is obligated to provide Authenticom with access to Reynolds' DMS systems. Authenticom frames this demand in the negative—e.g., that Reynolds must "stop blocking" Authenticom from accessing those systems—but the inescapable result of such a demand is that Reynolds must (in some fashion) do business with Authenticom. According to a wealth of well-established antitrust law, Authenticom's premise cannot stand.

It is axiomatic that the Sherman Act "'does not restrict the long recognized right of [a] trader or manufacturer engaged in an entirely private business, freely to exercise his own independent discretion as to parties with whom he will deal.'" *Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, LLP*, 540 U.S. 398, 408 (2004) (quoting *United States v. Colgate & Co.*, 250 U.S. 300, 307 (1919)); *see also Pac. Bell Tel. Co. v. Linkline Commc'ns, Inc.*, 555 U.S. 438, 448 (2009) ("As a general rule, businesses are free to choose the parties with whom they will deal, as well as the prices, terms, and conditions of that dealing.").

The Supreme Court decided *Trinko* to lay rest to the now unequivocal antitrust principle that "there is no duty to aid competitors." *Trinko*, 540 U.S. at 411. "There is a difference between

positive and negative duties, and the antitrust laws . . . have generally been understood to impose only the latter." *USM Corp. v. SPS Techs., Inc.*, 694 F.2d 505, 513 (7th Cir. 1982).

"[B]usinesses needn't acquiesce to every demand placed upon them by competitors or customers; their duties are negative – to refrain from anticompetitive conduct – rather than affirmative – to promote competition." *Greater Rockford Energy & Tech. Corp. v. Shell Oil Co.*, 790 F. Supp. 804, 821 (C.D. Ill. 1992), *aff'd*, 998 F.2d 391, 393 (7th Cir. 1993); *see also Morris Commc'ns Corp. v. PGA Tour, Inc.*, 364 F.3d 1288, 1296 (11th Cir. 2004) (emphasis omitted) ("Section 2 of the Sherman Act does not require [a firm] to give its product freely to its competitors."); *Foremost Pro Color, Inc. v. Eastman Kodak Co.*, 703 F.2d 534, 545 (9th Cir. 1983) (holding that a firm has no duty to "constrict[] product development so as to facilitate sales of rival products" or to help competitors "survive or expand").

"Enforced sharing" between competitors, moreover, requires courts to act as "central planners, identifying the proper price, quantity, and other terms of dealing—a role for which they are ill suited."[11] *Trinko*, 540 U.S. at 408; *see also Chic. Prof'l Sports Ltd. P'ship v. NBA*, 95 F.3d 593, 597 (7th Cir. 1996) ("[T]he antitrust laws do not deputize district judges as one-man regulatory agencies."); *Ball Mem'l Hosp. Inc. v. Mut. Hosp. Ins., Inc.*, 784 F.2d 1325, 1340 (7th Cir. 1986) (holding that courts should not "become little versions of the Office of Price Administration").

In *Aspen Skiing Co. v. Aspen Highlands Skiing Corp.*, 472 U.S. 585, 588 (1985), the Supreme Court outlined a limited exception to this general rule. For years, defendant, owner of

[11] For a more academic background on this principle, see Richard A. Posner, ANTITRUST LAW 242 (2d ed. 2001) ("Where the refusal to deal is unilateral, the only effective remedy is an order that defendant do business with the victim of the refusal to deal. The antitrust court becomes charged with the supervision of an ongoing commercial relationship, a function that courts *are not equipped to perform effectively*.") (emphasis added); *see also* Frank H. Easterbrook, *The Chicago School and Exclusionary Conduct*, 31 HARV. J.L. & PUB. POL'Y 439 (2008).

three of the four mountain ski resorts in Aspen, sold a joint pass with plaintiff, owner of the fourth mountain resort. *Id.* at 588-91. Defendant terminated the joint pass and refused even to sell lift tickets to the other owner at retail. *Id.* at 592-94. At the same time, defendant created its own pass for its three mountains and engaged in substantial marketing efforts that advertised its three mountains as the only places for skiing in the region. *Id.* at 594. As a result, plaintiff lost 50% of its market share over four years and lost substantial revenue for other skiing-related services. *Id.* at 594-95.

As the Supreme Court explained in *Trinko*, the Court in *Aspen* had imposed antitrust liability under Section 2 because the "unilateral termination of a voluntary (and thus presumably profitable) ***course of dealing*** suggested a willingness to forsake short-term profits to achieve an anticompetitive end" and "the defendant's unwillingness to renew the ticket even if compensated at retail price revealed a distinctly anticompetitive bent." *Trinko*, 540 U.S. at 409 (citing and explaining *Aspen Skiing*, 472 U.S. at 608-11) (emphasis added). Limiting *Aspen* to a prior course of dealing whose abrupt end evidenced anticompetitive intent, the Supreme Court stressed that "*Aspen Skiing* is at or near the outer boundary of § 2 liability." *Trinko*, 540 U.S. at 409; *see also Pac. Bell Tel.*, 555 U.S. at 448 (*Aspen Skiing* represents "limited circumstances in which a firm's unilateral refusal to deal with its rivals can give rise to antitrust liability").

Authenticom's Sherman Act Section 2 monopoly claim against Reynolds pleads itself right into dismissal under *Trinko* without any attempt to plead the limited exceptions of *Aspen Skiing*. Nor could Authenticom have pleaded such an exception. As acknowledged in the complaint, Reynolds sought to block and exclude Authenticom from the Reynolds enterprise software and computer system systematically over the past decade, culminating in almost

complete success by 2013. *See* Compl. ¶¶ 6, 7, 74, 189, 235. These allegations expressly plead Authenticom out of any *Aspen* exception.

Ultimately, Reynolds has no duty to deal with or to provide a right of access to Authenticom under *Trinko*. Indeed, the facts here are even more extreme, given that Authenticom demands such access without compensation. Authenticom's professed economic need for such access—and operational preference for automated access over the manual dealer push options allowed by Reynolds—does not change the analysis. This antitrust principle stands neatly in symmetry with Reynolds' absolute right to protect its computer system under the CFAA.[12] Authenticom's monopoly claim therefore must be dismissed on this basis.

ii. The Computer Fraud and Abuse Act protects a computer system owner's right to block and control access to its computer system

As set forth above, the CFAA prohibits acts of computer trespass by those who are not authorized users or who exceed authorized use. By definition, the CFAA allows the operator of a computer system to undertake certain means to protect its proprietary systems. Efforts to circumvent those means and obtain information are outlawed, under pain of criminal penalties and civil remedies. *See* 18 U.S.C. § 1030(a)(2)(C). As detailed in Section D(3) above, the Ninth

[12] To the extent that Authenticom categorizes Reynolds' unilateral decision to "close" its DMS platforms as a technical design change, its claim also fails. "'[C]ourts are properly very skeptical about claims that competition has been harmed by a dominant firm's product design changes.'" *Allied Orthopedic Appliances Inc. v. Tyco Health Care Grp. LP*, 592 F.3d 991, 998 (9th Cir. 2010) (quoting *United States v. Microsoft Corp.*, 253 F.3d 34, 65 (D.C. Cir. 2001)). Unless the challenged design serves *no purpose other than protecting a monopoly*, it is not actionable. *Id.* In contrast, "a design change that improves a product by providing a new benefit to consumers does not violate Section 2 absent some associated anticompetitive conduct." *Id.* at 998-99. Importantly, "[t]here is no room in this analysis for balancing the benefits or worth of a product improvement against its anticompetitive effects. If a monopolist's design change is an improvement, it is 'necessarily tolerated by the antitrust laws' unless the monopolist abuses or leverages its monopoly power in some other way when introducing the product." *Id.* at 1000 (citation omitted); *see also id.* at 1002 ("[A] monopolist has no duty to help its competitors survive or expand when introducing a new and improved product design."').

Circuit recently upheld such liability in *Facebook*, on facts materially indistinguishable from those admitted and pleaded by Authenticom here. *See* 844 F.3d at 1068. Again, the critical issue from the Ninth Circuit's perspective was the lack of authorization from the computer system owner: "Permission from the users alone was not sufficient to constitute authorization after Facebook issued the cease and desist letter." *Id.*

It is undisputed that Reynolds has not granted such authorization to Authenticom. The logical extension of Authenticom's claims is that computer owners can be compelled to grant such authorization under the antitrust laws. That is a radical proposition. In addition to creating a conflict between these two federal statutes, it also fundamentally contradicts virtually everything the U.S. Supreme Court and the Seventh Circuit have said about antitrust law in the last three decades. No case or court has ever suggested that the antitrust laws trump a computer owner's right to control access to that computer. That argument effectively requires a determination that Reynolds' system constitutes an essential facility—a standard that is lightyears away from being satisfied, pleaded, or applicable here. *See, e.g.*, *Blue Cross & Blue Shield United v. Marshfield Clinic*, 65 F.3d 1406, 1413 (7th Cir. 1995) (holding that a facility cannot be considered essential when it covers less than 50% of the relevant market); *Cyber Promotions, Inc. v. Am. Online, Inc.*, 948 F. Supp. 456, 464 (E.D. Pa. 1996) (holding that AOL's mechanism for blocking junk email was not sufficient to serve as a basis for an "essential facilities" claim because AOL customers could still access plaintiff's advertising products through other means); *see also Trinko*, 540 U.S. at 411 (questioning whether such a claim even exists). Authenticom satisfies none of these standards. And even if it did, a party seeking access to an essential facility can only obtain access—assuming it pleads all the other necessary elements for such a claim—on nondiscriminatory and commercially reasonable terms. *See, e.g.,*

MCI Commc'ns Corp. v. Am. Tel. & Tel. Co., 708 F.2d 1081, 1200 (7th Cir. 1983). Authenticom's demand for free and unfettered access to Reynolds' proprietary systems is hardly reasonable.

Authenticom's core problem is that Reynolds alone can authorize access to the DMS computer system and has chosen not to grant such access to Authenticom. Reynolds' fundamental right to exercise that choice is embedded within the CFAA as well as various other bodies of law, including basic property law. Nothing in Authenticom's Complaint, or the antitrust laws, overrides that principle.

iii. Authenticom has not and cannot plead a Kodak *"aftermarket" claim*

Kodak claims are rarely established, and Authenticom has not done so here. There is no actionable single-brand Reynolds-only market in "data integration" and no case has supported such a claim in circumstances like this.

To plead a monopolization claim Plaintiffs must allege plausible evidentiary facts suggesting: "(1) the possession of monopoly power in the relevant market and (2) the willful acquisition or maintenance of that power as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident." *United States v. Grinnell Corp.*, 384 U.S. 563, 570-71 (1966). Since Authenticom's complaint concedes that Reynolds has nothing close to monopoly power in the DMS market, Authenticom cannot and does not attempt to plead a plausible antitrust claim against Reynolds in any primary market. Instead, Authenticom attempts to plead an "aftermarket" monopoly claim.

"An aftermarket is a type of derivative market consisting of consumable goods or replacement components that must be used for the proper functioning of some primary good." Areeda & Hovenkamp ¶ 564b. As the name implies, aftermarkets involve goods or services

purchased after the primary product. Here, Authenticom alleges that the DMS serves as the primary product and that "dealer data integration" serves as the "aftermarket" product. Compl. ¶ 27.

The "economic presumption" is that aftermarket power is ordinarily constrained by competition in the primary market because "consumers make a knowing choice to restrict their aftermarket options when they decide in the initial (competitive) market" to make a purchase that restricts later choices. *Newcal Indus., Inc. v. IKON Office Solution*, 513 F.3d 1038, 1050 (9th Cir. 2008) (emphasis added). Accordingly, a fundamental predicate to an aftermarket claim is a plausible allegation that there is monopoly power — or no competition — in the primary market. *See id.*

In *Kodak*, the Supreme Court carved a limited exception to this presumption, holding that Kodak violated Section 2 of the Sherman Act by changing its policies mid-contract to require purchasers of its printers and copiers to also use its service for any repairs on printers. *Eastman Kodak Co. v. Image Tech. Services, Inc.*, 504 U.S. 451, 476 (1992).

Seventh Circuit Judge and noted antitrust scholar Hon. Frank Easterbrook has explained the peculiar and limited nature of the *Kodak* claim:

> What the Supreme Court held in [*Kodak*] is not that firms with market power are forbidden to deal in complementary products, but that they can't do this in ways that take advantage of customers' sunk costs. Kodak sold copiers that customers could service themselves (or through independent service organizations). Having achieved substantial sales, Kodak then moved to claim all of the repair work for itself. That change had the potential to raise the total cost of copier-plus-service above the competitive level—and, we observed in *Digital Equipment*, above the price that Kodak could have charged had it followed a closed-service model from the outset.

Schor v. Abbott Labs., 457 F.3d 608, 614 (7th Cir. 2006) (emphasis added).

Accordingly, in *Schor*, Judge Easterbrook refused to extend *Kodak*, holding "Schor does not accuse Abbott of any similar switch that would exploit customers' sunk costs; none is

possible in this market. Unless we generalize the Supreme Court's decision in [*Kodak*] to a rule against selling products that complement those in which the defendant has market power—which *Digital Equipment* already has held would be inappropriate—Schor is left without a leg to stand on." *Id.* at 614 (emphasis added); *see also Dig. Equip. Corp. v. Uniq Dig. Techs., Inc.*, 73 F.3d 756, 763 (7th Cir. 1996) ("The Court did not doubt in *Kodak* that if spare parts had been bundled with Kodak's copiers from the outset, or Kodak had informed customers about its policies before they bought its machines, purchasers could have shopped around for competitive life-cycle prices."); *Newcal*, 513 F.3d at 1048 ("[T]he critical distinction . . . was that the Kodak customers did not knowingly enter a contract that gave Kodak the exclusive right to provide parts and services for the life of the equipment.").[13]

Judge Easterbrook's explanation has come to famously reflect the unanimous agreement of the Supreme Court in *Kodak*: all nine Justices agreed that where purchasers have reasonable notice of what awaits them in the aftermarket, they cannot claim later that they were victims of an aftermarket monopoly under Section 2. *See Kodak*, 504 U.S. at 477 n.24 (majority opinion); *id.* 492 (Scalia, J., dissenting).

Authenticom fails to state a plausible "aftermarket" claim under Section 2 for several reasons.

---

[13] *See also DSM Desotech Inc. v. 3D Sys. Corp.*, 749 F.3d 1332, 1346 (Fed. Cir. 2014) ("Crucial to the *Kodak* decision . . . was the fact that customers had already purchased their equipment ***before*** learning about Kodak's policies on aftermarket parts and services.") (emphasis added); *PSI Repair Servs., Inc. v. Honeywell, Inc.*, 104 F.3d 811, 820 (6th Cir. 1997) ("By changing its policy ***after*** its customers were ***'locked in,'*** Kodak took advantage of the fact that its customers lacked the information to anticipate this change.") (emphasis added); *Newcal*, 513 F.3d at 1048 ("[T]he law prohibits an antitrust claimant from resting on market power that arises solely from contractual rights that consumers knowingly and voluntarily gave to the defendant . . . .") (emphasis omitted); *Universal Avionics Sys. Corp. v. Rockwell Int'l Corp.*, 184 F. Supp. 2d 947, 956 (D. Ariz. 2001), *aff'd*, 52 F. App'x 897 (9th Cir. 2002) (holding that plaintiff's claims failed because it could not demonstrate that its "customers were 'ignorant' at the time they purchased [defendant's] equipment").

First, Authenticom fails to allege that Reynolds has monopoly power in the primary antitrust market, because it asserts that Reynolds only has 30% share of the DMS market. *See* Compl. ¶ 33. By definition, this means Reynolds lacks monopoly power in the relevant primary antitrust market for a monopolization claim — i.e., the DMS market.

Second, Authenticom fails to allege any facts rebutting the economic presumption that any aftermarket power is not constrained by competition in the primary market of DMS platforms. Authenticom repeatedly claims that DMS platforms are "sticky" and that customers are unable to switch, but such a claim is not plausible. As this Court has already held, Reynolds has lost a third of its market share in the DMS market—decreasing from 40% to 28%—during the past decade. (Dkt. No. 172 at 6). Dealers are anything but "locked in" to the Reynolds enterprise software. (*See id.*).

Third, the "integration services" aftermarket is not an antitrust aftermarket as a matter of law under *Kodak* because the allegations in Authenticom's own complaint establish that dealers have had reasonable notice for at least a decade regarding Reynolds' closed computer system and the requirement that layered applications access the computer system only through the RCI interface and Reynolds Integration Hub. *See* Compl. ¶ 6; *see also id.* nn.6, 10-11, 13 (citing news articles from 2006-2011 all reflecting Reynolds' policy). For better or worse, Reynolds' closed system has been the *sine qua non* of Reynolds in the marketplace for over a decade. Some dealers appreciate Reynolds' policy; some dealers dislike it; and some are likely indifferent, but by the terms of the pleading itself, every dealership that has licensed a Reynolds enterprise software computer system for the past decade has known about its "closed" nature. Under *Kodak*, this knowledge precludes the aftermarket from serving as the relevant antitrust market for a Section 2 claim.

Relatedly, Authenticom fails to meet *Kodak*'s requirement of alleging that Reynolds changed its policies after dealers entered into their contracts. Authenticom knows that precisely the opposite is true: every current Reynolds customer signed its DMS contract with full knowledge of Reynolds' bar on third-party access and hostile data integrators like Authenticom. As Authenticom itself pleads, Reynolds' stance has been widely known in the automotive industry since at least 2007. *See, e.g.*, Compl. ¶ 6.

Ultimately, it is not an antitrust monopoly violation for Reynolds to design and build a closed computer system that it believes necessary for its model of performance, integrity, and security. And having built that system to the investment of billions of dollars, it is not a Sherman Act Section Two monopoly violation to protect it. Reynolds has the absolute discretion to grant or deny access to anyone it chooses for any reason or no reason at all pursuant to *Trinko*, *Facebook*, and *Kodak*. Nor is it an appropriate antitrust remedy to require Reynolds to grant authorized computer access pursuant to any single third party's preferred business wishes. The law imposes no such duty on Reynolds, DMS providers, or any other computer systems operator.

Thus, Authenticom's Section 2 claim against Reynolds must be dismissed.

3. Authenticom Fails to State a Claim Based on Any Vertical Restraints (Second and Third Causes of Action)

Finally, Authenticom's vertical restraint allegations likewise do not plausibly state a claim. Authenticom alleges that Reynolds uses *per se* unlawful tying and exclusive dealing provisions in its contracts with dealers in violation of Section 1 of the Sherman Act. Specifically, Authenticom alleges that Reynolds is using its market power in the tying market (i.e., DMS platforms) to unreasonably restrain competition in the tied product market (i.e., dealer integration services). Compl. ¶¶ 263-64. Similarly, Authenticom alleges that Reynolds is using

exclusive dealing provisions in its contracts with vendors and dealers to preclude Authenticom from having access to dealer data. *Id.* ¶¶ 254-55.

These theories of liability are not plausible and should be dismissed. First, as a preliminary matter, the alleged vertical restraints are not *per se* unlawful but are analyzed under the antitrust Rule of Reason, which balances anticompetitive effects against procompetitive justifications. Second, Authenticom fails to state a proper tying claim, by definition, because the buyer of the primary products (i.e., dealers that purchase DMS platforms) are not the same buyers of the tied product (i.e., third party vendors that pay for integration services). Third, Authenticom fails to allege the facts necessary to suggest that the alleged exclusive dealing arrangements with dealers and vendors fall within the ambit of U.S. antitrust law. Finally, even at the pleadings stage, Authenticom fails to allege sufficient facts showing these vertical arrangements cannot be considered as reasonable when analyzed under the Rule of Reason. For all of these reasons, Authenticom's second and third causes of action should be dismissed.

i. Vertical restraints fall under the antitrust "Rule of Reason"

As a matter of law, Authenticom fails to allege a *per se* unlawful tying claim because it alleges that Reynolds only has a 30 percent share of the market for the tying product. *See* Compl. ¶ 33. In order for an alleged tying arrangement to be analyzed under the *per se* rule, Reynolds must have "market power" for the tying product (i.e., DMS platforms) such that it can "appreciably restrain free competition" in the alleged market for the tied product (i.e., dealer integration services). *N. Pac. Ry. Co. v. United States*, 356 U.S. 1, 6 (1958). The Supreme Court has held that market share of 30 percent does not demonstrate the requisite market power necessary to apply the *per se* rule to a tying claim.[14] *Jefferson Parish Hosp. Dist. No. 2 et al. v.*

[14] Other courts have reinforced the Supreme Court's decision in *Jefferson Parish. See, e.g.*, *Dickson v. Microsoft Corp.*, 309 F.3d 193, 209-10 n.20 (4th Cir. 2002); *Grappone, Inc. v. Subaru*

Hyde, 466 U.S. 2, 13-14 (1984). Accordingly, any alleged tying by Reynolds must be analyzed under the rule of reason.[15]

Exclusive dealing relationships, as well, are treated under the rule of reason.[16] *See, e.g., Roland Mach. Co. v. Dresser Indus., Inc.*, 749 F.2d 380, 393 (7th Cir. 1984). Recognizing that exclusive dealing may have procompetitive effects and may be motivated by goals that are not anticompetitive, the Supreme Court has never treated exclusive dealing arrangements as *per se* unlawful. In fact, in *Jefferson Parrish*, the concurring Justices stressed that the challenged vertical restraint was not a *per se* unreasonable form of exclusive dealing because the firm at issue only had 30 percent market share. *See Jefferson Parrish*, 466 U.S. at 46 (Brennan, J., concurring).[17]

Furthermore, the *per se* rule has been specifically rejected when applied to vertical restraints relating to product integration in computer software platform markets, even when the software provider has near-monopoly power in the tying product. In *United States v. Microsoft Corp.*, 253 F.3d 34, 89 (D.C. Cir. 2001), the United States challenged Microsoft's integration of

---

of New England, Inc., 858 F.2d 792, 797 (1st Cir. 1988); *Med. Alert Ambulance v. Atl. Health Sys.*, 2007 U.S. Dist. LEXIS 57083, at *25-27 (D.N.J. 2007).

[15] Again, as this Court has already recognized, Reynolds has *lost* a third of its market share in the DMS market—decreasing from 40% to 28%—during the past decade. (Dkt. No. 172 at 6).

[16] Authenticom also conceded in their briefing for the preliminary injunction that its exclusive dealing claim must be evaluated under the rule of reason. (Dkt. No. 51 at 28).

[17] Since *Jefferson Parrish*, courts have actually held that much higher levels of market power are necessary to establish an exclusive dealing claim that is *per se* unlawful. *See, e.g.*, *Sterling Merch., Inc. v. Nestle, S.A.*, 656 F.3d 112, 123-24 (1st Cir. 2011) (holding that courts should apply the rule of reason to an exclusive dealing arrangement when market share is less than 30 or 40 percent because market foreclosure levels are unlikely to be of concern); *see also Sewell Plastics v. Coca-Cola Co.*, 720 F. Supp. 1186, 1212-14 (W.D.N.C. 1988) (holding that market share of 40% was not sufficient to sustain an exclusive dealing claim), *aff'd*, 912 F.2d 463 (4th Cir. 1990).

its PC operating system (the tying product) with its Internet Explorer browser product (the tied product). Despite Microsoft's dominant **80%** market share of the operating system market, the D.C. Circuit refused to apply the *per se* rule to any software-to-software tying claim. *See id.* at 90. The court recognized that tying of such products "may produce efficiencies that courts have not previously encountered and thus the Supreme Court had not factored into the *per se* rule as originally conceived." *Id.* at 93.

These considerations led the *Microsoft* court to one conclusion: "we cannot comfortably say that bundling in platform software markets has so little 'redeeming virtue,' and that there would be so 'very little loss to society" from its ban, that 'an inquiry into its costs in the individual case [can be] considered [] unnecessary.'" *Id.* at 94 (internal citations omitted). In other words, the court held that the rule of reason is the appropriate way to evaluate tying arrangements where the tying product is software and the tied product is complementary software functionality. *Id.* at 95.

At the end of the day, Reynolds lacks the requisite market power as a matter of law for any of the alleged tying or exclusive dealing restraints to be analyzed under the *per se* rule. *See, e.g., Batson v. Live Nation Entm't, Inc.*, 746 F.3d 827, 831 (7th Cir. 2014). Authenticom has failed to plead any vertical *per se* claims.

ii. There is no tying because different buyers purchase the alleged tying product (DMS) and tied product (integration interfaces)

A tying arrangement is "defined as an agreement by a party to sell one product but only on the condition that the buyer also purchases a different (or tied) product, or at least agrees that he will not purchase that product from any other supplier." *N. Pac. Ry. Co. v. United States*, 356 U.S. 1, 5-6 (1958); *see also A.O. Smith Corp. v. Lewis, Overbeck & Furman*, 979 F.2d 546, 547 (7th Cir. 1992).

The seller must condition its sale of one product on its selling of a second product to the same buyer. *See Jefferson*, 466 U.S. at 12 ("[T]he essential characteristic of an invalid tying arrangement lies in the seller's exploitation of its control over the tying product to force the buyer into the purchase of a tied product that the buyer either did not want at all, or might have preferred to purchase elsewhere on different terms."); Areeda & Hovenkamp ¶ 1752b ("There is no tie for any antitrust purpose unless the defendant improperly imposes conditions that explicitly or practically require buyers to take the second product if they want the first one.").

While auto dealers license DMS platforms from Reynolds; application vendors license integration interfaces from Reynolds. *See* Compl. ¶¶ 59-60. There is, therefore, no tying arrangement by definition: Authenticom has failed even to allege that Reynolds is using "market power" over DMS enterprise software to compel auto dealers who purchase that software to also purchase Reynolds application interfaces. Simply put, dealers don't buy those interfaces. And any amount they may pay for that service is an indirect cost dependent on whether, and how much, the application provider may be able to pass through to the dealer.[18]

iii. Authenticom has not alleged actionable exclusive dealing under antitrust laws

Authenticom alleges that Reynolds engages in two levels of exclusive dealing: (1) restricting auto dealerships from allowing outside access to the Reynolds enterprise software and computer system without Reynolds authorization; and (2) requiring application developers to access the Reynolds DMS through the Reynolds Integration Hub. *See* Compl. ¶ 255.

[18] Authenticom's argument that vendors "pass through" any integration costs to dealers does not save this claim. No case has ever permitted such a circular reasoning; doing so would explode the realm of conduct covered by U.S. antitrust law and would contradict the principles of antitrust standing articulated in *Illinois Brick Co. v. Illinois*, 431 U.S. 720 (1977) (holding that indirect victims of an alleged antitrust violation have no standing to sue).

To state a plausible exclusive dealing claim, Authenticom must plausibly allege: (1) the exclusive dealing "is likely to keep at least one significant competitor of the defendant from doing business in a relevant market"; and (2) "the probable (not certain) effect of the exclusion will be to raise prices above (and therefore reduce output below) the competitive level, or otherwise injure competition." *Roland Mach.*, 749 F.2d at 394.[19]

Authenticom has not alleged either of these things. First, Authenticom makes no allegation that it cannot continue serving the market of DMS platforms that allow screen scrapers to access the systems (e.g., DealerTrack). Indeed, Authenticom admits that it is currently providing those services with respect to certain Reynolds-owned applications. *See* Compl. ¶ 207.

Critically, Authenticom's own allegations (and the Reynolds DMS contracts) also betray the theory that Reynolds has contractually barred its dealers from "using Authenticom's data integration services." Compl. ¶ 232. As defined by the Seventh Circuit, "Exclusive dealing occurs when a supplier and a distributor agree that the distributor will carry only that supplier's products." *Roland Mach.*, 749 F.2d at 392. None of Reynolds' contracts fall into that category, even by analogy. Reynolds' sole contractual restriction is on Authenticom (and other third parties) directly accessing its DMS. Authenticom is free to (and does) receive data from Reynolds dealers in numerous other ways, including through dealer-pushed Dynamic Reports. *See* Compl. ¶ 105. The mere fact that Authenticom dislikes this restriction and views it as an inferior method of receiving data does not establish an exclusive dealing contract. *See, e.g.*, *SCFC ILC, Inc. v. Visa USA, Inc.*, 36 F.3d 958, 972 (10th Cir. 1994) ("Surely, if its goal is to

[19] "The exclusion of one or even several competitors, for a short time or even a long time, is not *ipso facto* unreasonable. The welfare of a particular competitor who may be hurt as the result of some trade practice is the concern not of the federal antitrust laws. . . . The exclusion of competitors is cause for antitrust concern only if it impairs the health of the competitive process itself." *Roland Mach.*, 749 F.2d at 394 (citing *Products Liability Ins. Agency, Inc. v. Crum & Forster Ins. Cos.*, 682 F.2d 660, 663-65 (7th Cir. 1982)) (emphasis added).

compete more effectively in that market, we do not believe this objective constitutes the proverbial sparrow the Sherman Act protects."). Similarly, nothing in Reynolds' RCI agreement restricts application vendors from using Authenticom to pull data from other DMS providers—which comprise over 70% of the market. *See generally* Ex. 3. Indeed, Reynolds does not even provide any "integration services" with respect to that majority-share of the market. *See* Compl. ¶ 102 n.24. And the fact that CDK independently decided not to allow Authenticom to access its DMS does not affect the legality of Reynolds' vertical contracts—most of which were in effect long before CDK made that decision. Authenticom has not, therefore, been excluded by Reynolds from the relevant market for purposes of its exclusive dealing claim.[20]

Second, Authenticom makes insufficient allegations to show that the effect of the exclusion is to raise prices above the "competitive level." The fact that Reynolds' prices might be higher than Authenticom's prices is not probative of an injury to competition. Authenticom uses its own prices as a benchmark, but as established above, Authenticom is able to do so only because it enjoys illegal, free access to Reynolds' DMS and the resources therein. Digital music

[20] Authenticom does not allege that the relevant market for purposes of exclusive dealing is product specific. Even if it did, however, such an allegation would make no difference as relevant markets generally cannot be limited to a single manufacturer's products. *See, e.g.*, *PSKS, Inc. v. Leegin Creative Leather Prods. Inc.*, 615 F.3d 412, 418 (5th Cir. 2010) (rejecting relevant product market limited to a single brand), cert. denied, 131 S. Ct. 1476 (2011); *Green Country Food Mkt. v. Bottling Grp.*, 371 F.3d 1275, 1283 (10th Cir. 2004) (holding that Pepsi products are not a relevant market); *Tanaka v. Univ. of S. Cal.*, 252 F.3d 1059, 1065 (9th Cir. 2001) ("By attempting to restrict the relevant market to a single athletic program in Los Angeles based solely on her own preferences, [plaintiff] has failed to identify a relevant market for antitrust purposes."); *Elliott v. United Ctr.*, 126 F.3d 1003, 1004-06 (7th Cir. 1997) (affirming dismissal of vendor's claim against stadium because single arena food sales could not, as matter of law, qualify as relevant market). And under the exception, Authenticom fails to allege that Reynolds' DMS platforms constitute their own market because "'the commodity is unique, and therefore not interchangeable with other products.'" *Coast to Coast Entm't, LLC v. Coastal Amusements, Inc.*, No. 05-cv-3977-MLC, 2005 WL 7979273, at *18 (D.N.J. Nov. 7, 2005) (*quoting Queen City Pizza, Inc. v. Domino's Pizza, Inc.*, 124 F.3d 430, 439 (3d Cir. 1997)).

is cheaper on piracy sites that steal the songs and sell them, versus legitimate sites that pay license fees to artists and recording labels, for a reason. The pirates have very different costs.

For these reasons, Authenticom's exclusive dealing claims fail as a matter of law.

iv. Rule of Reason analysis

Vertical arrangements like tying and exclusive dealing are evaluated under the antitrust rule of reason. *See, e.g.*, *Batson v. Live Nation Entm't, Inc.*, 746 F.3d 827, 831 (7th Cir. 2014); *Roland Mach. Co. v. Dresser Indus., Inc.*, 749 F.2d 380, 393 (7th Cir. 1984).

Reynolds' conduct can be a basis for antitrust liability only if it cannot be explained by "valid business reasons." *Kodak*, 504 U.S. at 483 (internal quotations omitted); *see also Viamedia, Inc. v. Comcast Corp.*, 16-cv-5486, 2017 WL 698681, at *4 (N.D. Ill. Feb. 22, 2017) ("[P]laintiffs seeking to establish an unlawful refusal to deal must show that the defendant's actions serve no rational procompetitive purpose.").

Authenticom has failed to state a plausible antitrust claim that is evaluated under the rule of reason — that is, one where Reynolds' action "serves no rational procompetitive purpose." In effect, what Authenticom has alleged is that Reynolds vertically integrated certain data functionalities into its DMS system. "Vertical integration is a universal feature of economic life and it would be absurd to make it a suspect category under the antitrust laws just because it may hurt suppliers of the service that has been brought within the firm." *Jack Walters & Sons Corp. v. Morton Bldg., Inc.*, 737 F.2d 698, 710 (7th Cir. 1984). As Judge Posner emphasized: "vertical integration usually is procompetitive." *Id.* And as the court emphasized in *Microsoft*, that is especially true in the software arena. *See Microsoft Corp.*, 253 F.3d at 89.

Authenticom admits that Reynolds has consistently blocked hostile integrators to ensure system security on its DMS platforms. *See* Compl. ¶ 235. Authenticom itself acknowledges that such goals are not irrational, stating "[p]rotecting the security of the dealer data is ***critically***

important and the responsibility of all entities involved." *Id.* ¶ 62 (emphasis added). Authenticom tries to wave these security concerns away by claiming that Authenticom itself, in 2017, provides a secure product. *Id.* ¶ 240. But that says nothing about the rationality of Reynolds' decision to close its system—in 2007—based on the risks posed by third party access in general. Moreover, disagreement over the specific methods that Reynolds chose to enhance the privacy, security, and performance of its system is immaterial. *See, e.g.*, *VBR Tours, LLC v. Nat'l R.R. Passenger Corp.*, 2015 WL 5693735, at *9 (N.D. Ill. Sept. 28, 2015) ("[T]he question is not whether [the defendant] chose the most competitive offer but whether it had any procompetitive purpose. It is not whether [the defendant] optimally (or even prudently or competently) exercised its business judgment but whether it had any valid business reason."). Even a monopolist has "the right to redesign its products to make them more attractive to buyers whether by reason of lower manufacturing cost and price or improved performance," and need not "constrict[] its product development so as to facilitate sales of rival products." *California Computer Products, Inc. v. Int'l Bus. Machines Corp.*, 613 F.2d 727, 744 (9th Cir. 1979). So too does Reynolds.

To sustain a claim based on its vertical restraint allegations, Authenticom must plausibly allege that Reynolds' conduct is not supported by any valid business reason. It has failed to do so. Accordingly, even at the pleading stage, this Court must reject Authenticom's tying and exclusive dealing claims under a rule of reason analysis.

F. Authenticom's Tortious Interference Claim Is Based on Illegal and Void Contracts

In addition to its antitrust claims, Authenticom also pleads that Reynolds has tortiously interfered with Authenticom's contracts. *See* Compl. ¶¶ 277-286. The assertedly-breached

contracts are Authenticom's agreements with dealerships that use Reynolds' DMS and with vendors that want to receive data from Reynolds' DMS. *See id.* ¶ 280.

As set forth above, to assert a claim for tortious interference, Authenticom must show that its contracts are valid and enforceable. *See, e.g.*, *Behnke v. Hertz Corp.*, 235 N.W.2d 690, 692 (Wis. 1975). But Authenticom's contracts, and the performance they call for, are illegal with respect to Reynolds' DMS under the CFAA, the WCCA, and multiple other statutes and bodies of law. Authenticom's claims for interference with those contracts should therefore be dismissed. *See, e.g.*, *Stamatiou v. U.S. Gypsum Co.*, 400 F. Supp. 431, 435 (N.D. Ill. 1975), *aff'd*, 534 F.2d 330 (7th Cir. 1976).

The illegality of Authenticom's contracts establishes a second legal bar to its tortious interference claims. Under Wisconsin law, a required element of a tortious interference claim is that "the defendant must not have been justified or privileged to interfere." *Select Creations, Inc. v. Paliafito Am. Inc.*, 911 F. Supp. 1130, 1156 (E.D. Wis. 1995). The illegality of Authenticom's contracts is one form of valid privilege. *See id.* at 1159 (discussing this type of privilege, and others); RESTATEMENT (SECOND) OF TORTS § 773. Given the illegality of Authenticom's contracts (and Reynolds bona fide belief in that illegality), any actions by Reynolds that interfered with those contracts (and the performance thereof) was therefore privileged. Authenticom's tortious interference claims should be dismissed on this basis as well.

G. Authenticom's Claim for Tortiously Interfering Statements Is Not Properly Pleaded Against Reynolds

Authenticom also pleads that Reynolds committed tortious interference by making allegedly "false" statements about Authenticom. *See* Compl. ¶ 280. But Authenticom does not support this claim with any specific allegations about the false statements Reynolds supposedly made. In paragraph 204 of the Complaint, Authenticom quotes a statement made by CDK about

third party integrators.[21] But no comparable statements by Reynolds are ever pleaded or identified. Without pleading what the allegedly false statements are, who made them, when they were made, who they were made to, and why they were false and affected Authenticom's business, the conclusory allegation against Reynolds cannot stand. It should therefore be dismissed. *See Twombly*, 550 U.S. at 555 (holding that "a formulaic recitation of the elements of a cause of action will not do").

H. Injunctive Relief Is Inappropriate Here

Authenticom's request for injunctive relief remains legally inappropriate and barred under multiple doctrines and rules of law.

First and foremost is the rule that injunctions cannot be issued that permit or further illegal conduct. *See, e.g.*, *Shondel v. McDermott*, 775 F.2d 859, 868 (7th Cir. 1985) ("An obviously sensible application of this principle [of unclean hands] is to withhold an equitable remedy that would encourage, or reward (and thereby encourage), illegal activity, as where the injunction would aid in consummating a crime[.]"). Indeed, the U.S. Supreme Court has held that a district court cannot even conduct the usual balance-of-harms analysis when considering behavior (in that case, the sale of medical marijuana) that Congress has prohibited by statute. *See United States v. Oakland Cannabis Buyers Co-op*, 532 U.S. 483, 497 (2001) ("A district court cannot, for example, override Congress' policy choice, articulated in a statute, as to what behavior should be prohibited."). The Seventh Circuit has likewise held that forcing a company to do business with a rival that has wronged it in the past is, itself, a form of irreparable harm. *See Original Great Am. Chocolate Chip Cookie Co., Inc. v. River Valley Cookies, Ltd.*, 970 F.2d

[21] The statements from CDK do not support Authenticom's claim either, given that the statements in question refer only to data integrators generally and say nothing about Authenticom specifically.

273, 277 (7th Cir. 1992) (Posner, J.) (holding that a preliminary injunction imposed real, unquantifiable, and irreparable harm on a party forced to continue doing business with a franchisee that had previously committed breach of contract and trademark infringement).

In addition, injunctive relief is inappropriate here given (1) the bar on excessive delay,[22] (2) the extraordinarily high (and not met) standards for granting a mandatory injunction, (3) the far greater risks and burdens that an injunction imposes on Reynolds, as weighed under the balance of harms analysis; (4) Authenticom's use of an allegedly impending bankruptcy largely of its own making to manufacture an "irreparable harm," and (5) the fact that Authenticom's claims have no chance of success on the merits, for at least all the reasons set forth above.

IV. CONCLUSION

For the reasons set forth above, Reynolds moves that Authenticom's claims each be dismissed. And because the deficiencies in those claims—most particularly the illegality of Authenticom's efforts to access Reynolds' DMS without authorization—cannot be cured by amendment, Reynolds requests that the dismissal be with prejudice.

---

[22] Authenticom affirmatively pleads that it waited over two years from when it learned of the alleged conspiracy before filing suit. *See* Compl. ¶ 181. There is extensive authority, including from the Seventh Circuit and the Western District of Wisconsin, holding that a two-year delay in seeking relief defeats any possible showing of irreparable harm. *See, e.g.*, *Jones v. Markiewicz-Qualkinbush*, 842 F.3d 1053, 1060, 1062 (7th Cir. 2016) (district court "was on solid ground" in determining that plaintiffs' "delay in bringing suit was 'the most important driver of the decision'" to deny a preliminary injunction; plaintiffs "could have acted" at least three months sooner); *Ty, Inc. v. Jones Grps., Inc.*, 237 F.3d 891, 902-03 (7th Cir. 2001) ("Delay in pursuing a preliminary injunction may raise questions regarding the plaintiff's claim that he or she will face irreparable harm if a preliminary injunction is not entered."); *Essentia Health v. Gundersen Lutheran Health Sys., Inc.*, No. 17-CV-100-WMC, 2017 WL 1318112, at *8 (W.D. Wis. Apr. 7, 2017) (Conley, J.) (finding plaintiff's claim of "irreparable harm" was "weak" and "insufficient" given two-year delay in seeking relief against defendant's ongoing conduct) (citation omitted); *see also, e.g.*, *Carson Grp., Inc. v. Davenport*, No. 16-CV-10520, 2016 WL 7212522, at *7 (N.D. Ill. Dec. 13, 2016) (denying preliminary injunction where plaintiff knew about alleged illegal conduct in January 2016 but did not bring suit until the following November); *Ohr v. Arlington Metals Corp.*, 148 F. Supp. 3d 659, 673-74 (N.D. Ill. 2015) (denying preliminary injunction where plaintiff delayed 15 months before seeking relief).

DATED: July 21, 2017

Respectfully submitted,

/s/ *Aundrea K. Gulley*

John S. Skilton
JSkilton@perkinscoie.com
Charles G. Curtis, Jr.
CCurtis@perkinscoie.com
Michelle M. Umberger
MUmberger@perkinscoie.com
Brandon M. Lewis
BLewis@perkinscoie.com
Jesse J. Bair
JBair@perkinscoie.com
PERKINS COIE LLP
One East Main Street, Suite 201
Madison, WI 53703
Telephone: 608-663-7460
Facsimile: 608-663-7499

Kathleen A. Stetsko
KStetsko@perkinscoie.com
PERKINS COIE LLP
131 South Dearborn St., Suite 1700
Chicago, IL 60603
Telephone: 312-324-8400
Facsimile: 312-324-9400

Kathy Patrick
kpatrick@gibbsbruns.com
Aundrea K. Gulley
agulley@gibbsbruns.com
Brian T. Ross
bross@gibbsbruns.com
Brice A. Wilkinson
bwilkinson@gibbsbruns.com
Ross M. MacDonald
rmacdonald@gibbsbruns.com
GIBBS & BRUNS, LLP
1100 Louisiana, Suite 5300
Houston, Texas 77002
Telephone: 713-650-8805
Facsimile: 713-750-0903

Michael P.A. Cohen
MCohen@sheppardmullin.com
Amar S. Naik
ANaik@sheppardmullin.com
SHEPPARD MULLIN RICHTER & HAMPTON LLP
Suite 100
2099 Pennsylvania Avenue, N.W.
Washington, D.C. 20006
Telephone: 202-747-1900
Facsimile: 202-747-1901

Attorneys for Defendant
The Reynolds and Reynolds Company